XKEYSCORE Workflows

05 March 2009

What is a workflow?

- Workflows automate queries.
  - One-time
  - Standing
- Every search type can be a workflow.
  - Same functionality and capability
- Follow on actions
  - Email alert
  - Download actions
  - Metadata summary

Who can submit a workflow?

- Anyone!
- One owner per workflow
  - Multiple-users can be notified
- If ownership needs to be changed, a ticket can be submitted to the team.
- Future: sharing workflows
  - Right now, only the owner has the results in their “My Results” view.

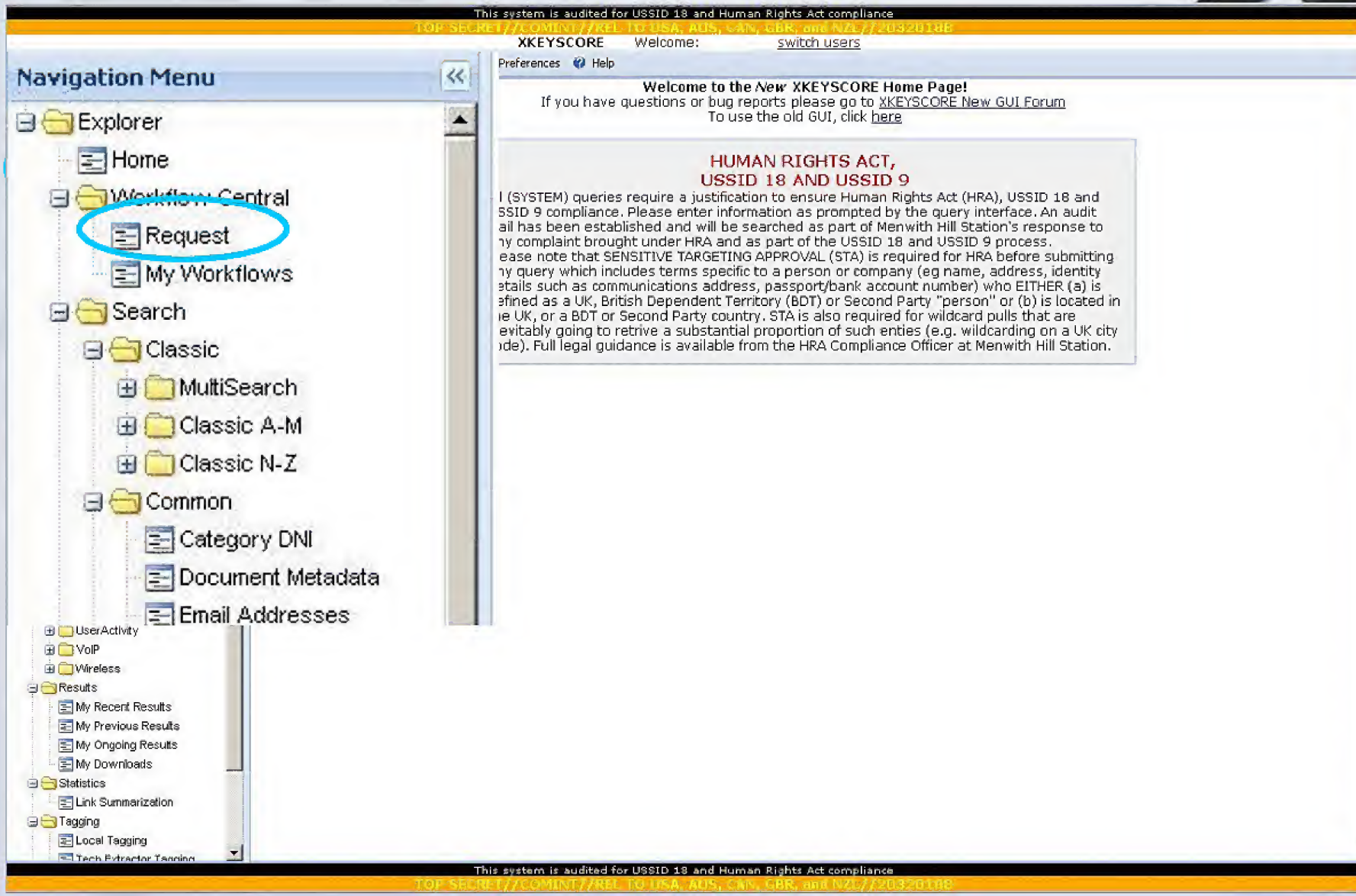
What can I do with a workflow?

- Workflows can be configured to run once
- Workflows can be configured to run daily
  - Every 1, 2, 3, 4, 6, 8, 12 or 24 hours
  - You can set an offset to start running at a certain hour
- Download results
- Email results and email alerts
- MAILORDER results
- MySQL report

Why do I want a workflow?

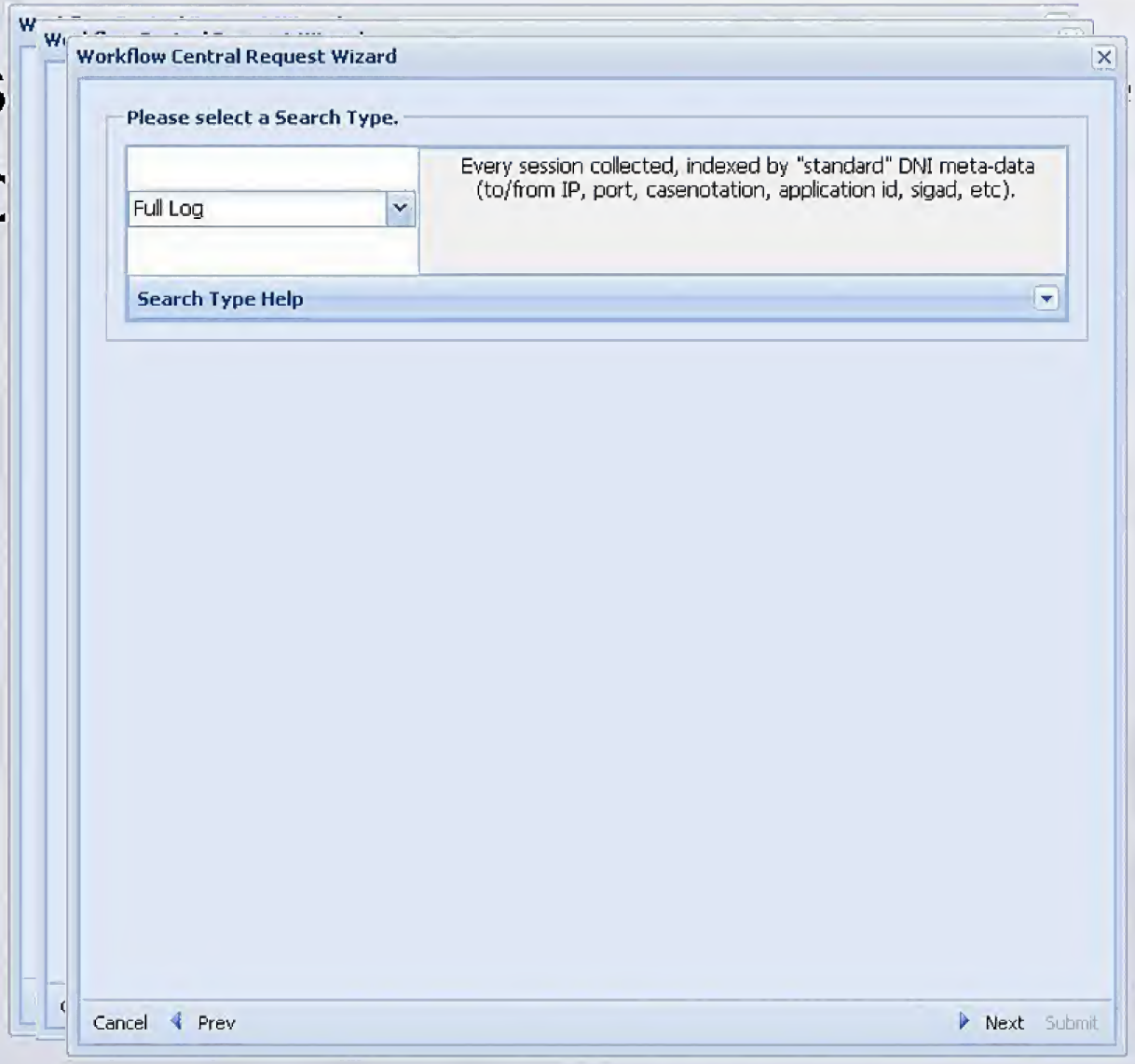
- XKEYSCORE has a rolling buffer of data
- Repetitive queries
- Sigdev purpose
  - Fingerprint and appid testing
- Queries take a long time during high times
- Follow on actions
  - Google Earth data
  - Statistics
  - Customizable – write a script!

How do I setup a workflow?



How do I setup a workflow?

First, s a workflc



How do I setup a workflow?

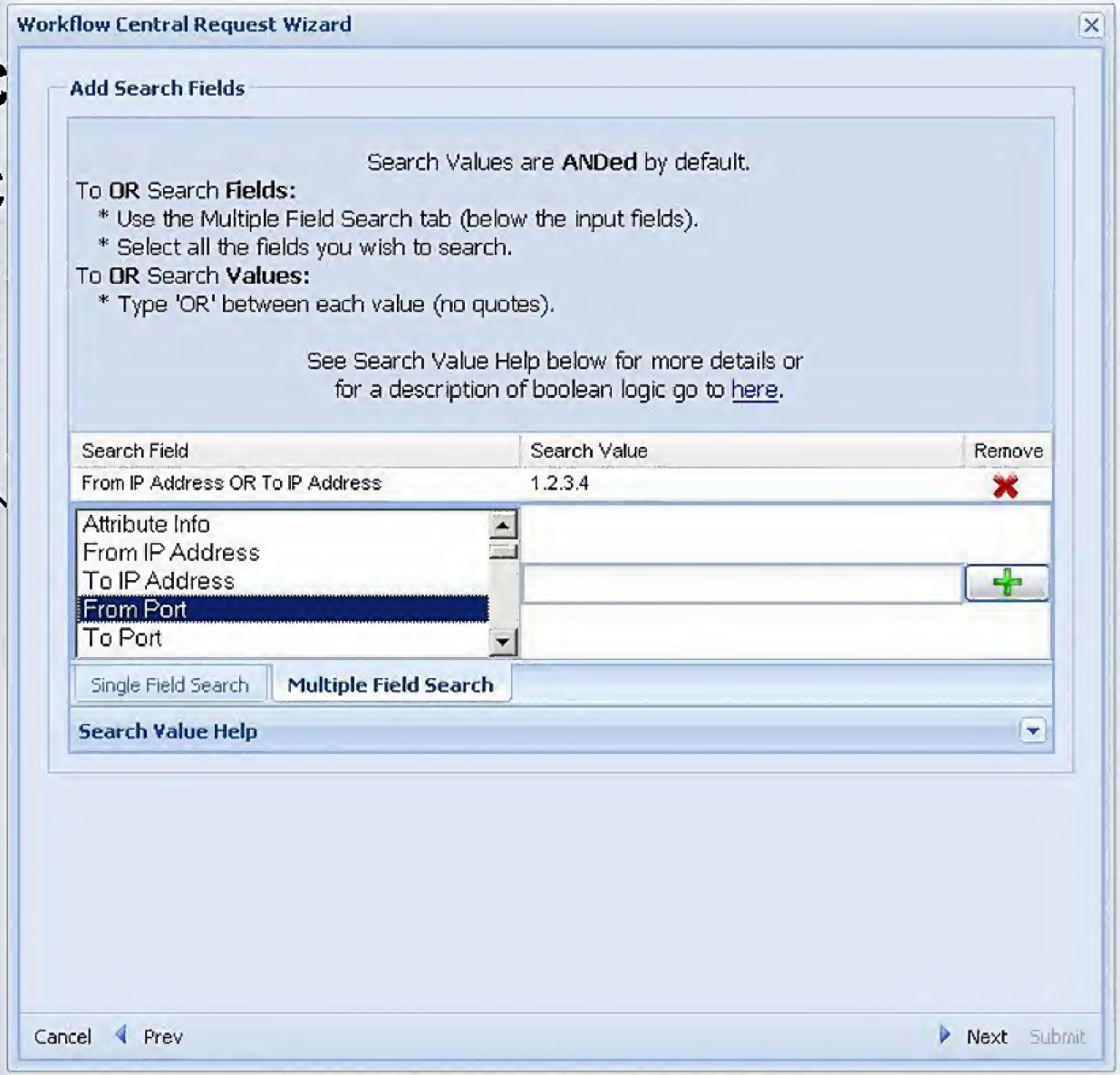
ring or one-

ıst be unique per user
must have a justification
justifications

How do I setup a workflow?

Selec ant to
searc

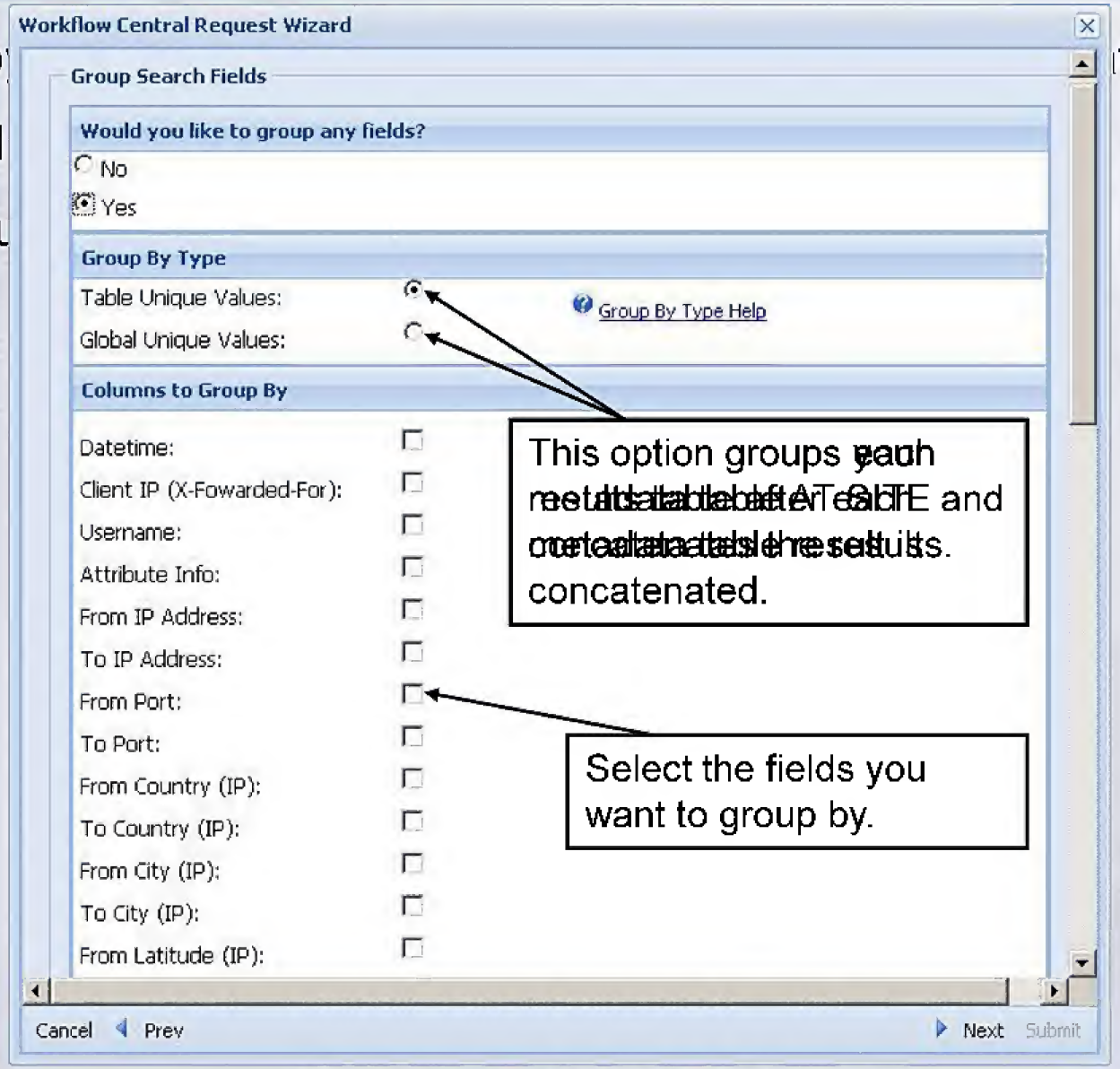
Select a field to search



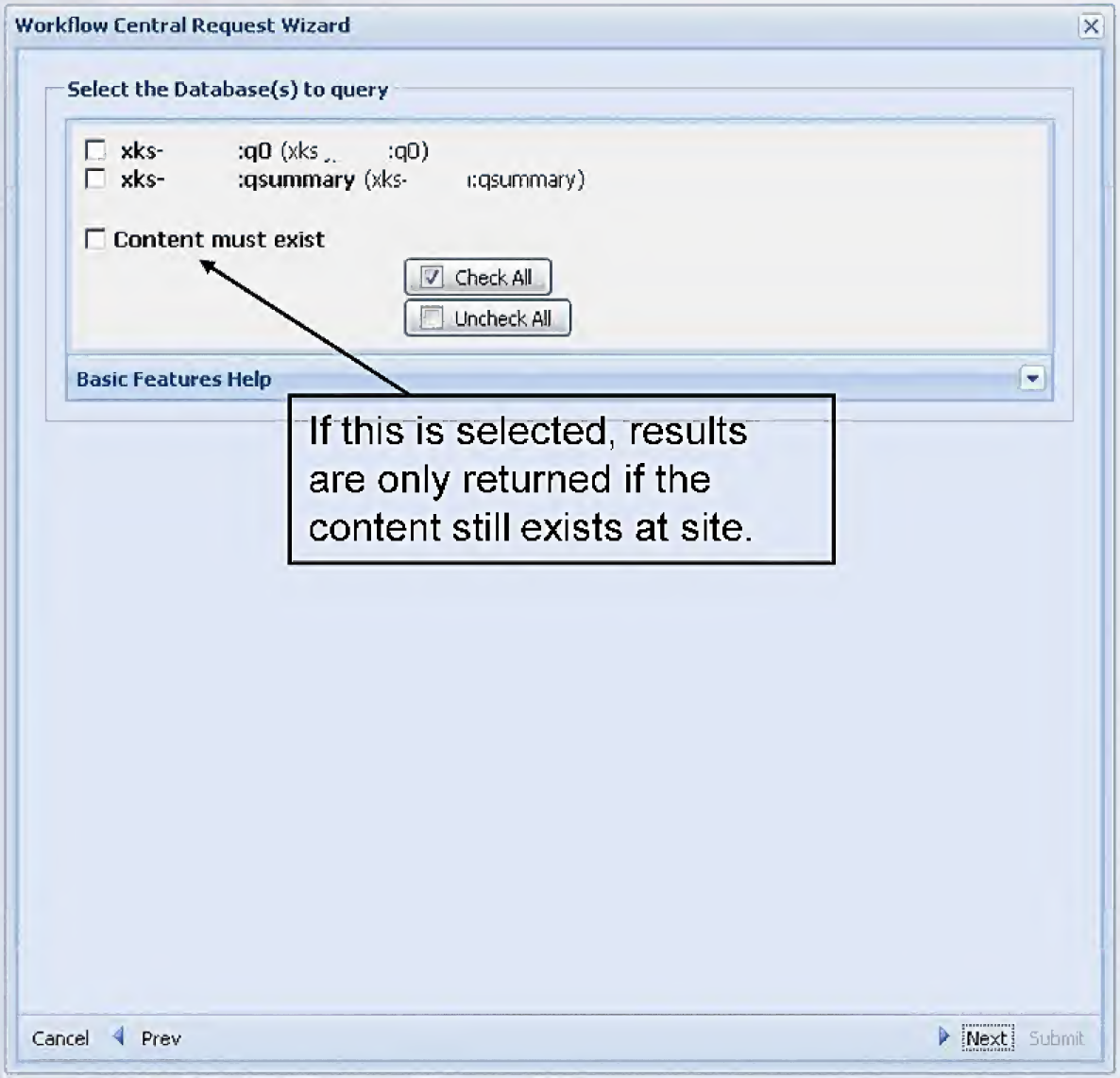
or every field, ou must select ıe PLUS key

Group by option

- Group b… …ta results.
  - Red…
  - Retu…

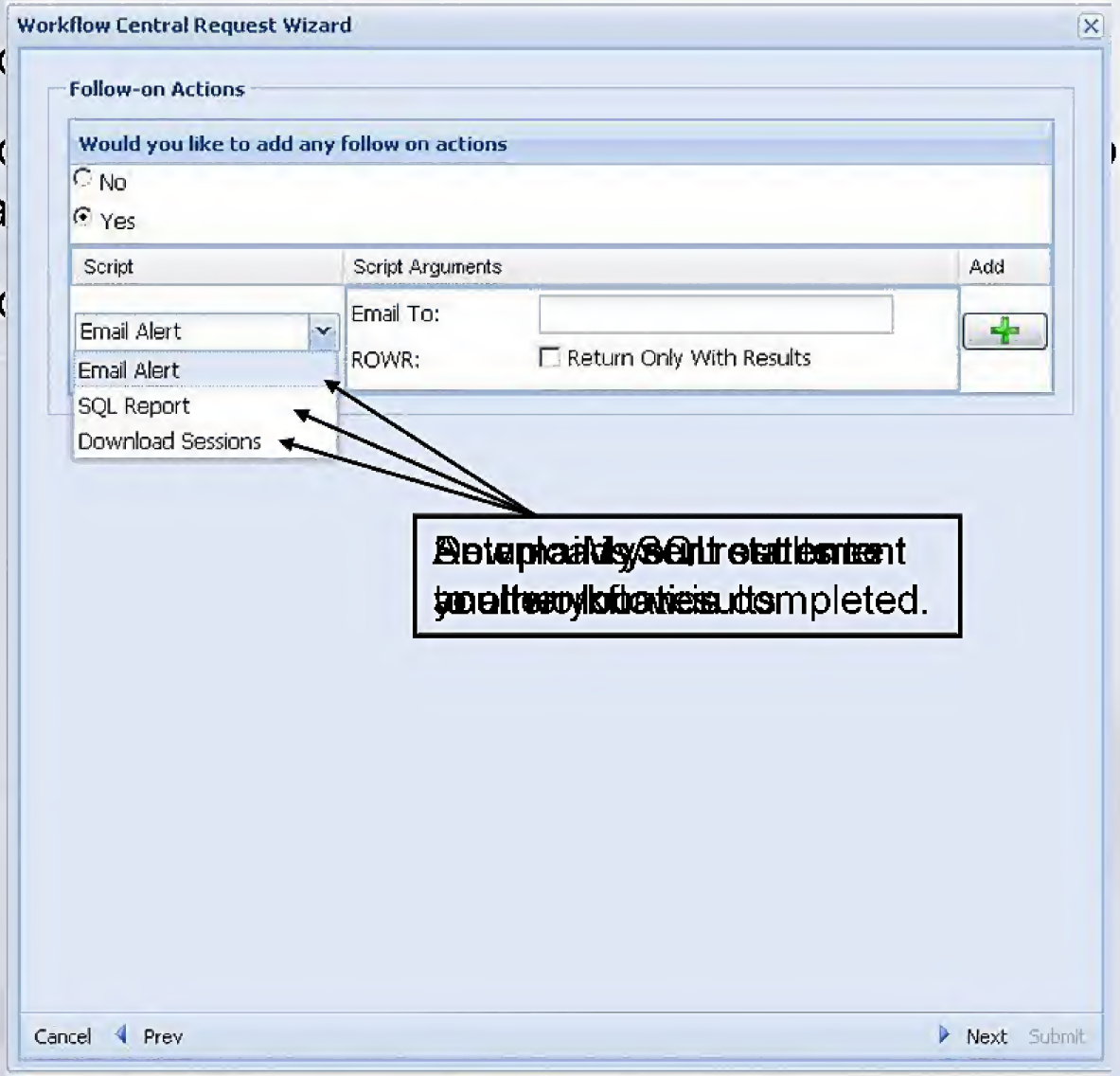


Select databases

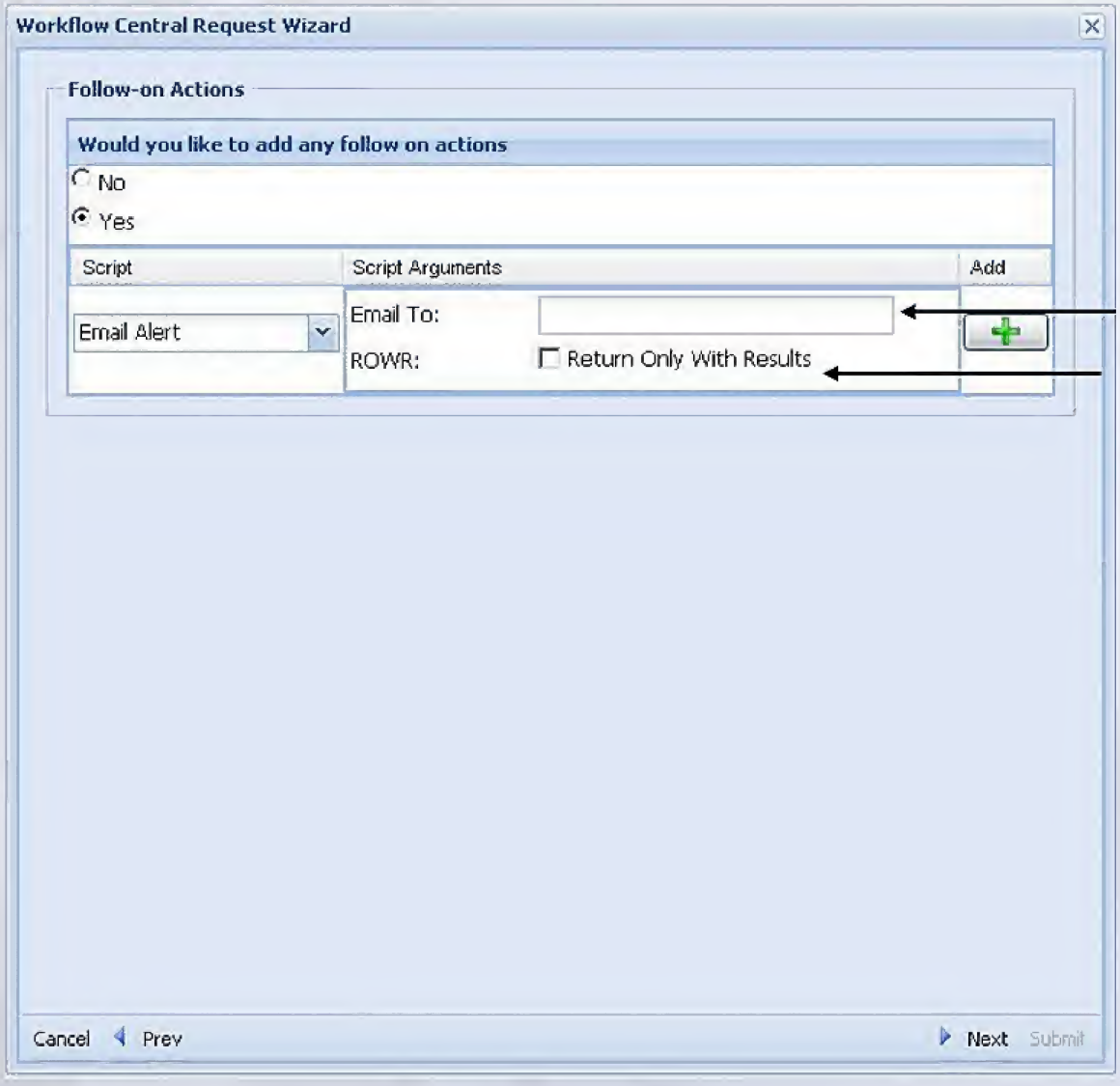


Follow on Actions

- All
- All ntent) to another loca
- All



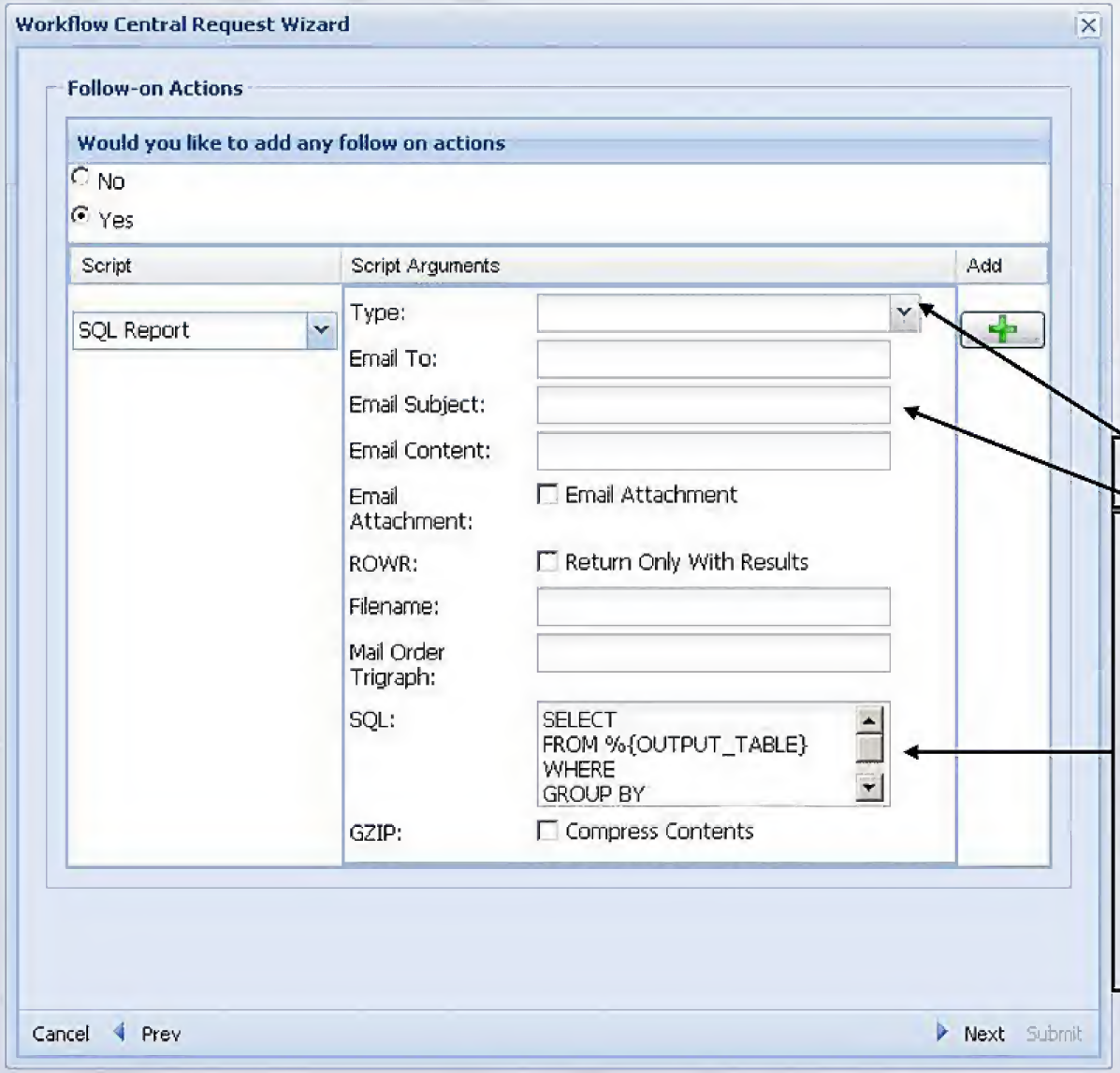
Email alert



Comma delimited email addresses.

This option only sends an email if you workflow has results.

SQL report



CSV or HTML

This must be a VALID SQL statement.

Email metadata that a user can set.

Example.

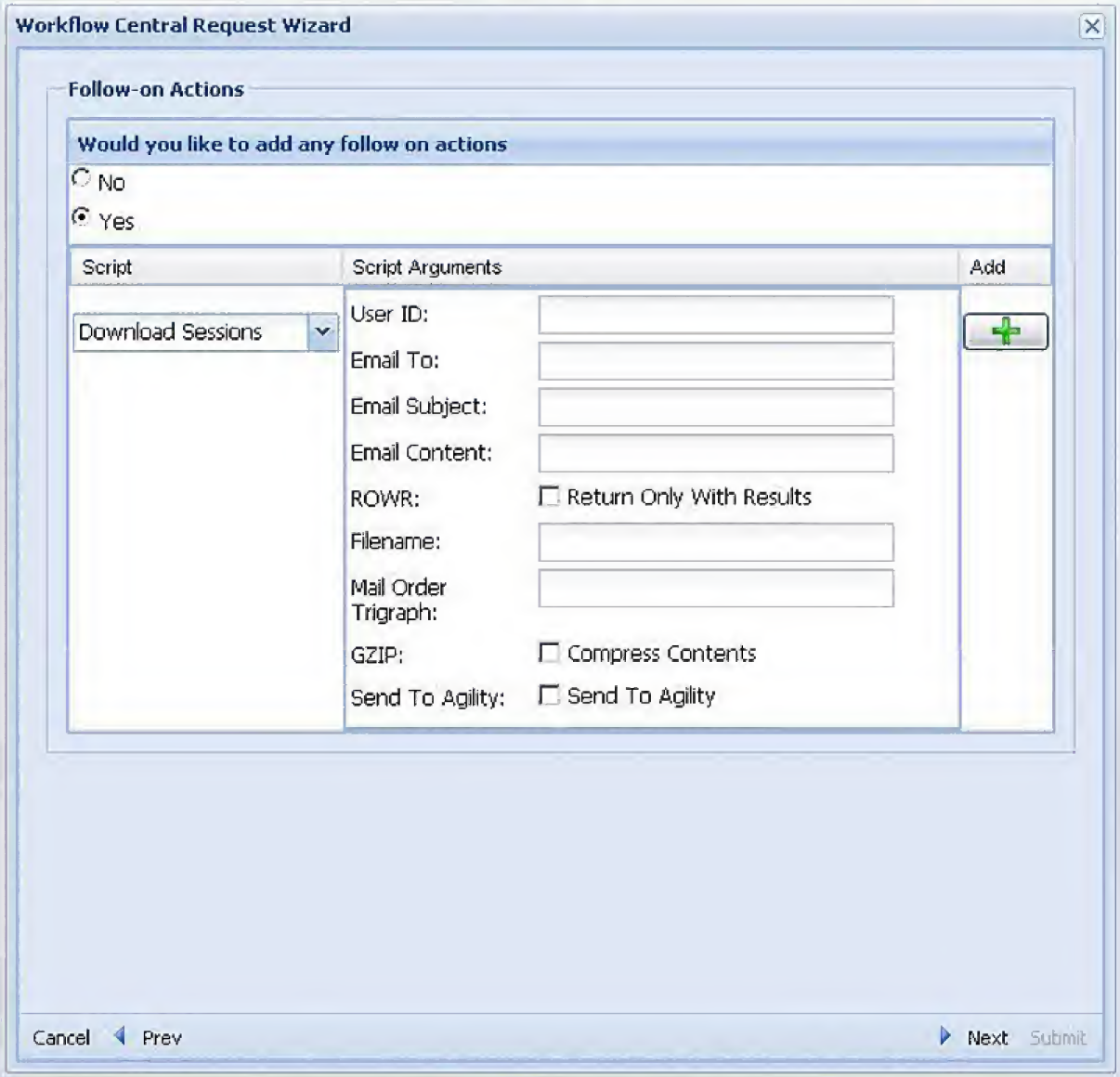
SELECT casenotation, sigad

FROM %{OUTPUT_TABLE}

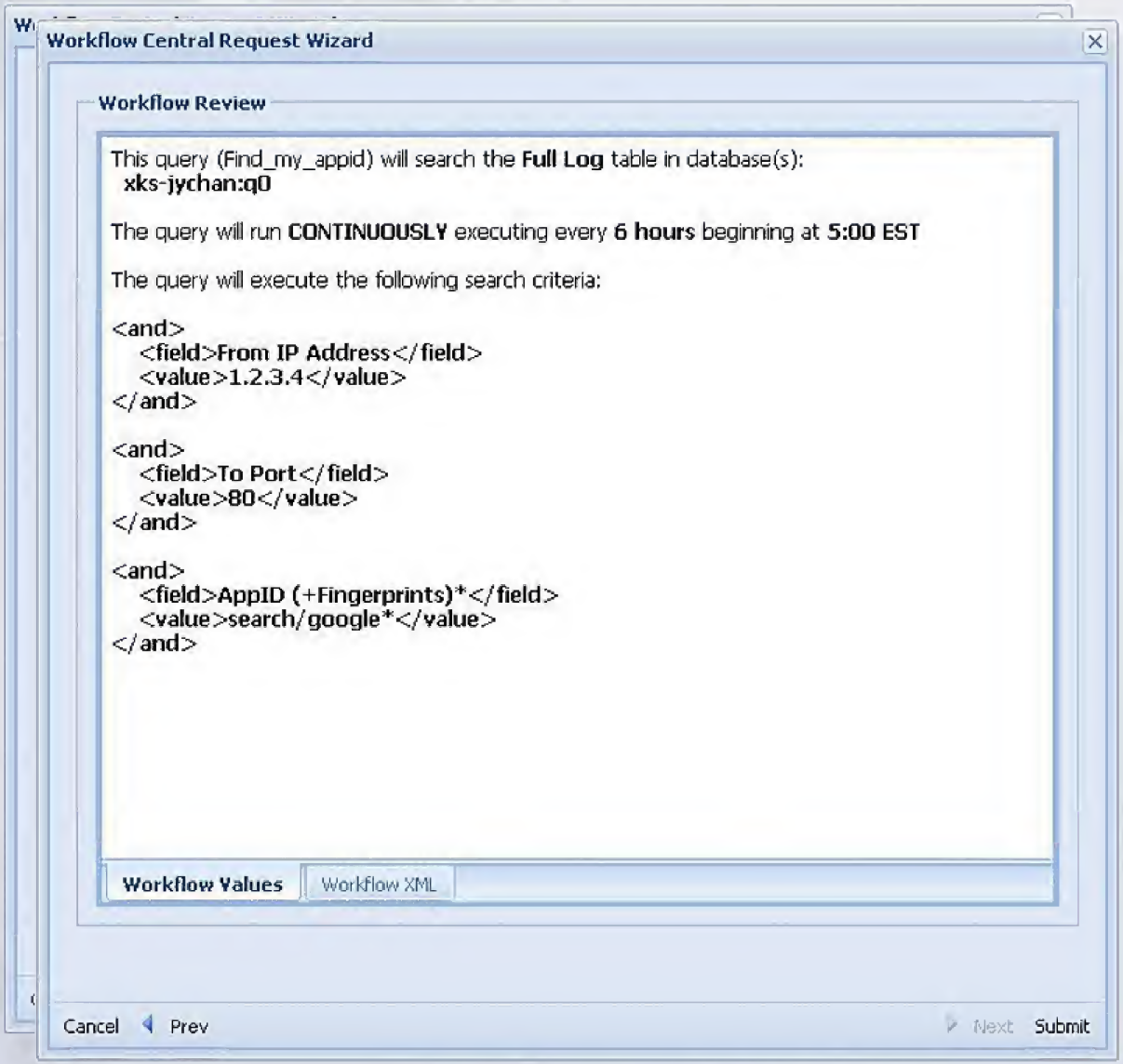
WHERE sigad!=''

GROUP BY casenotation

Download Results

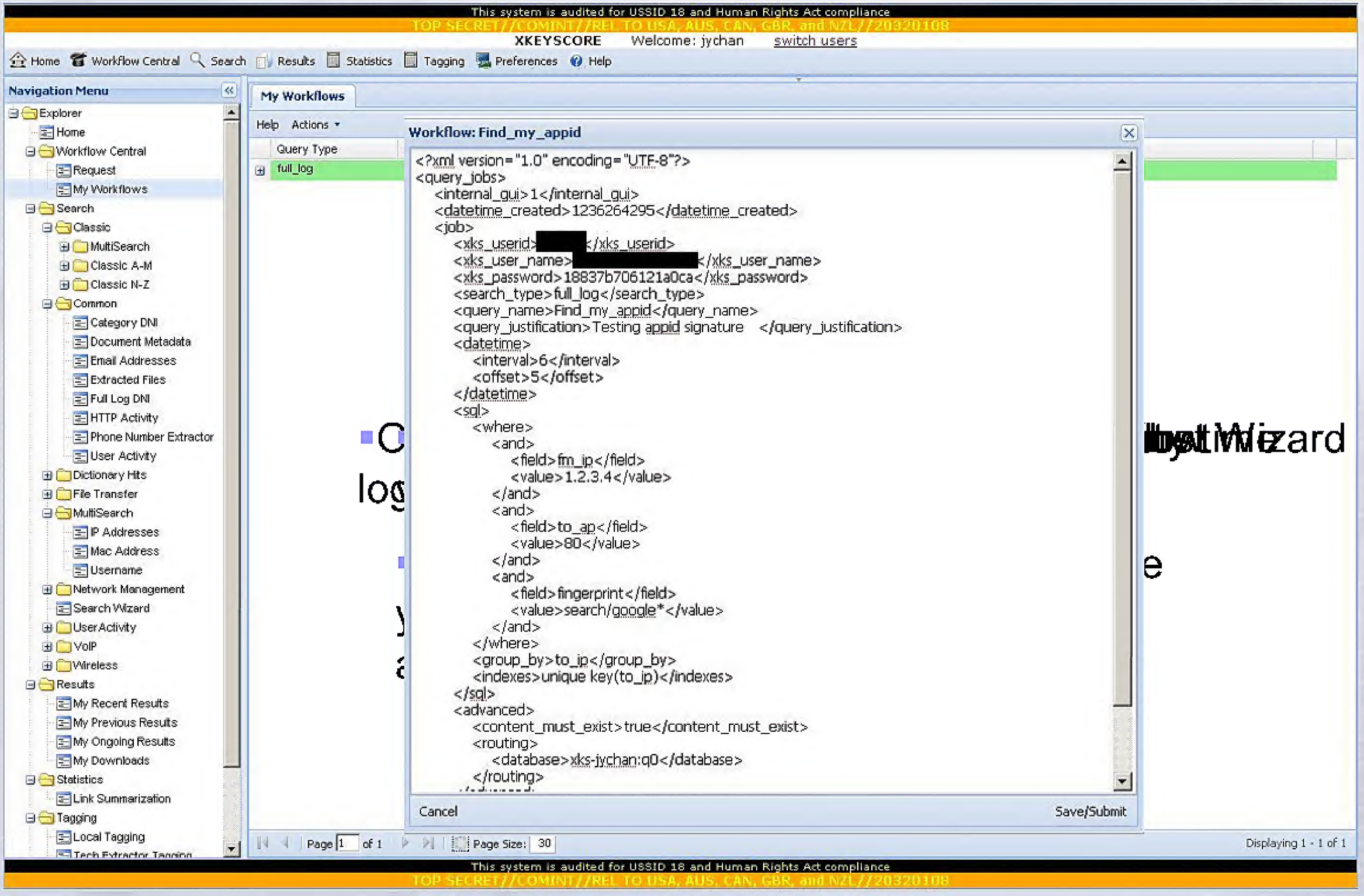


You're almost done!



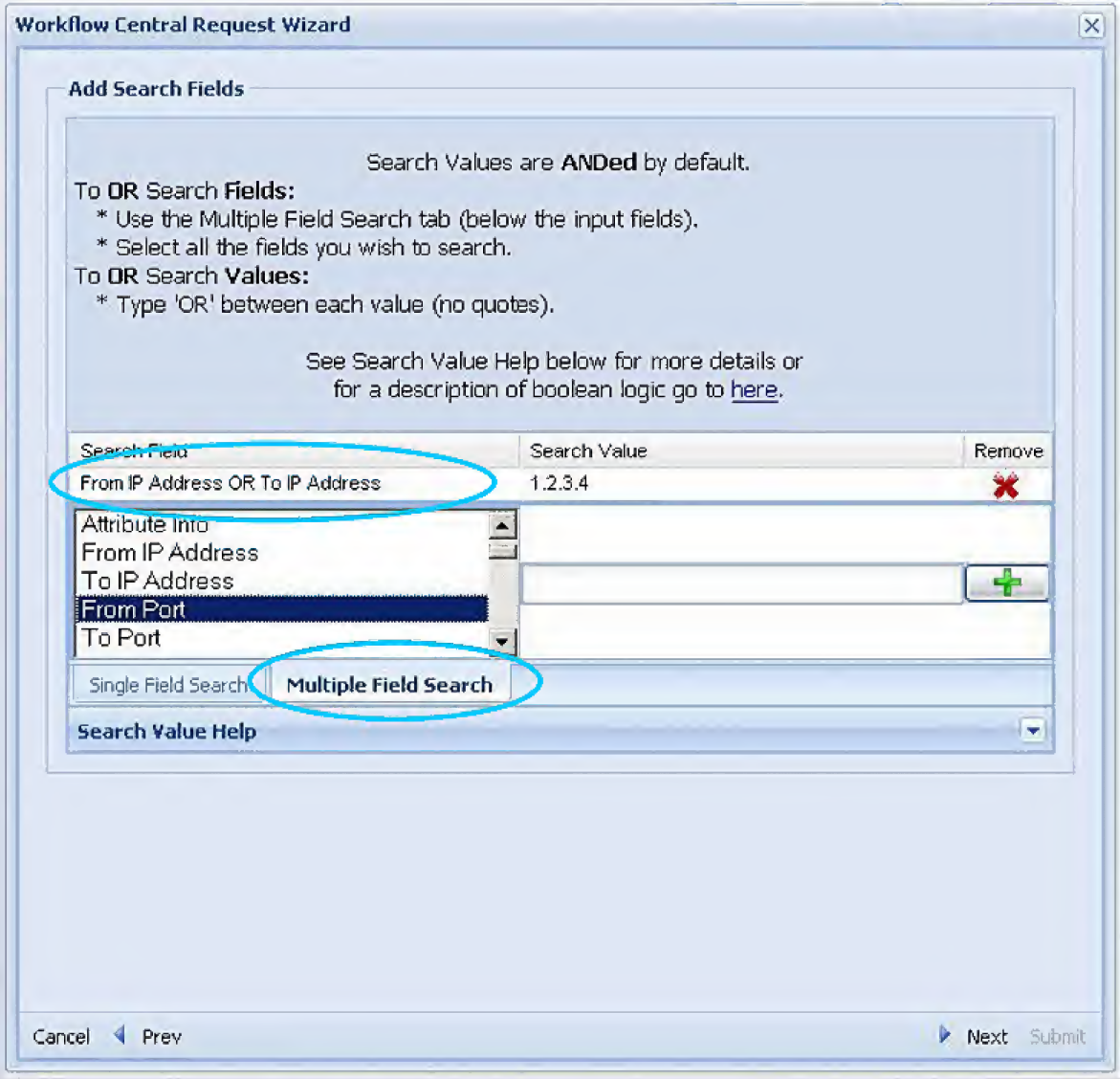
Workflow Pending

Workflow Approved



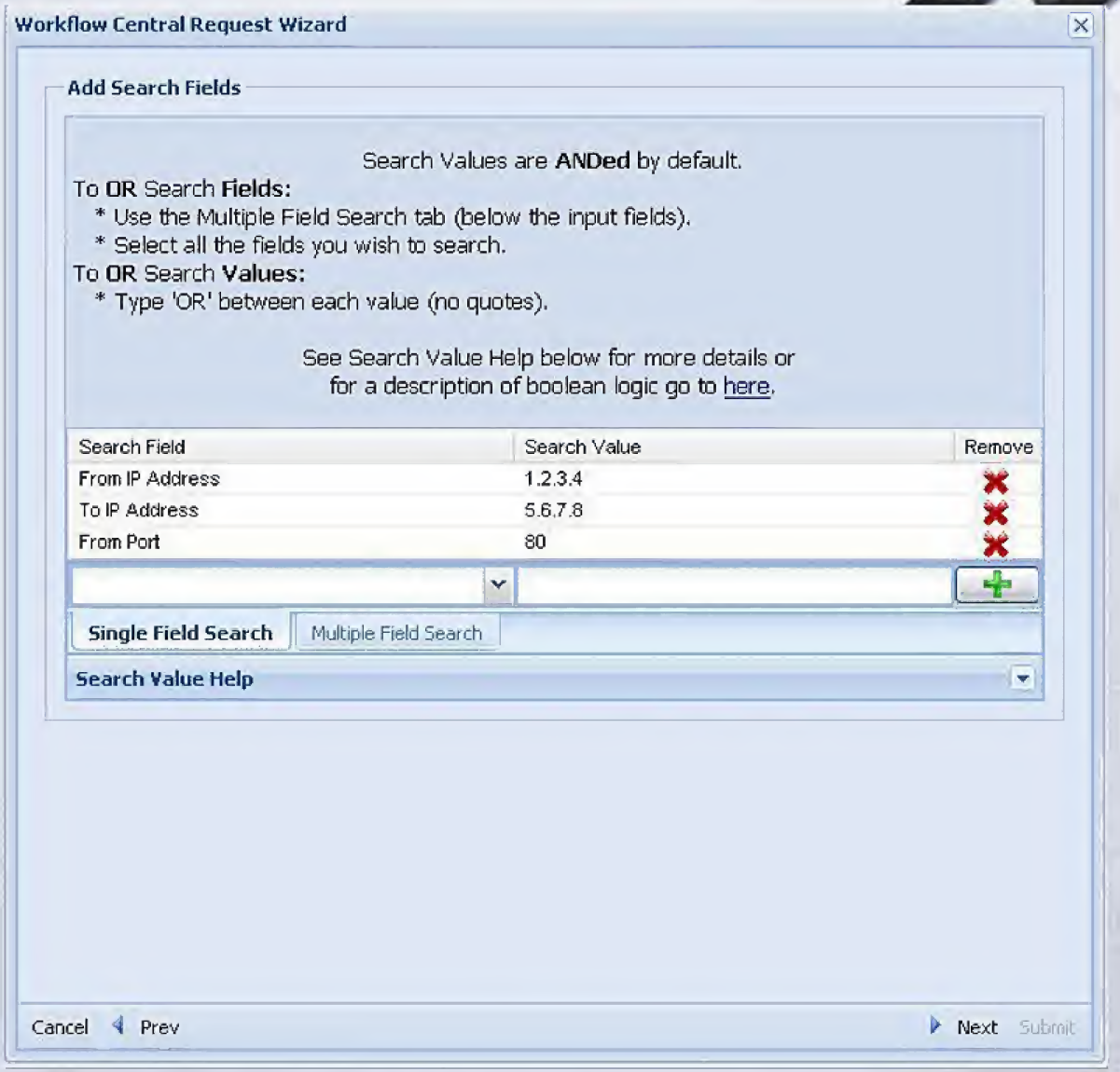
Common mistakes

- From IP and To IP with the same value.
- In this view, terms are ANDed together.
- Use Multiple Field Search Tab.



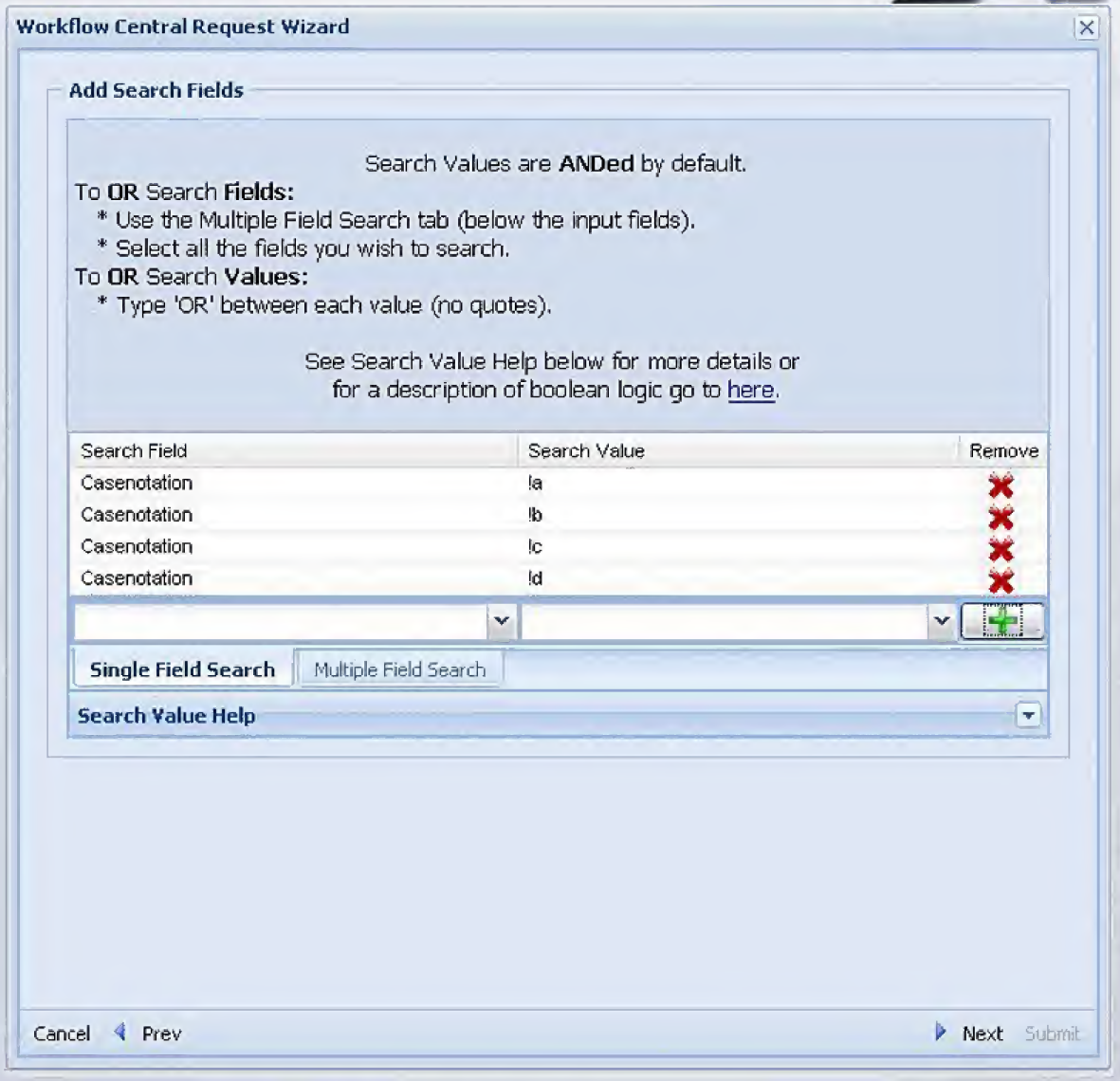
Common mistakes

- Using the multiple field search does not break this up into 3 search<->value pairs.
- Enter each term separately in the singe fieldsearch.

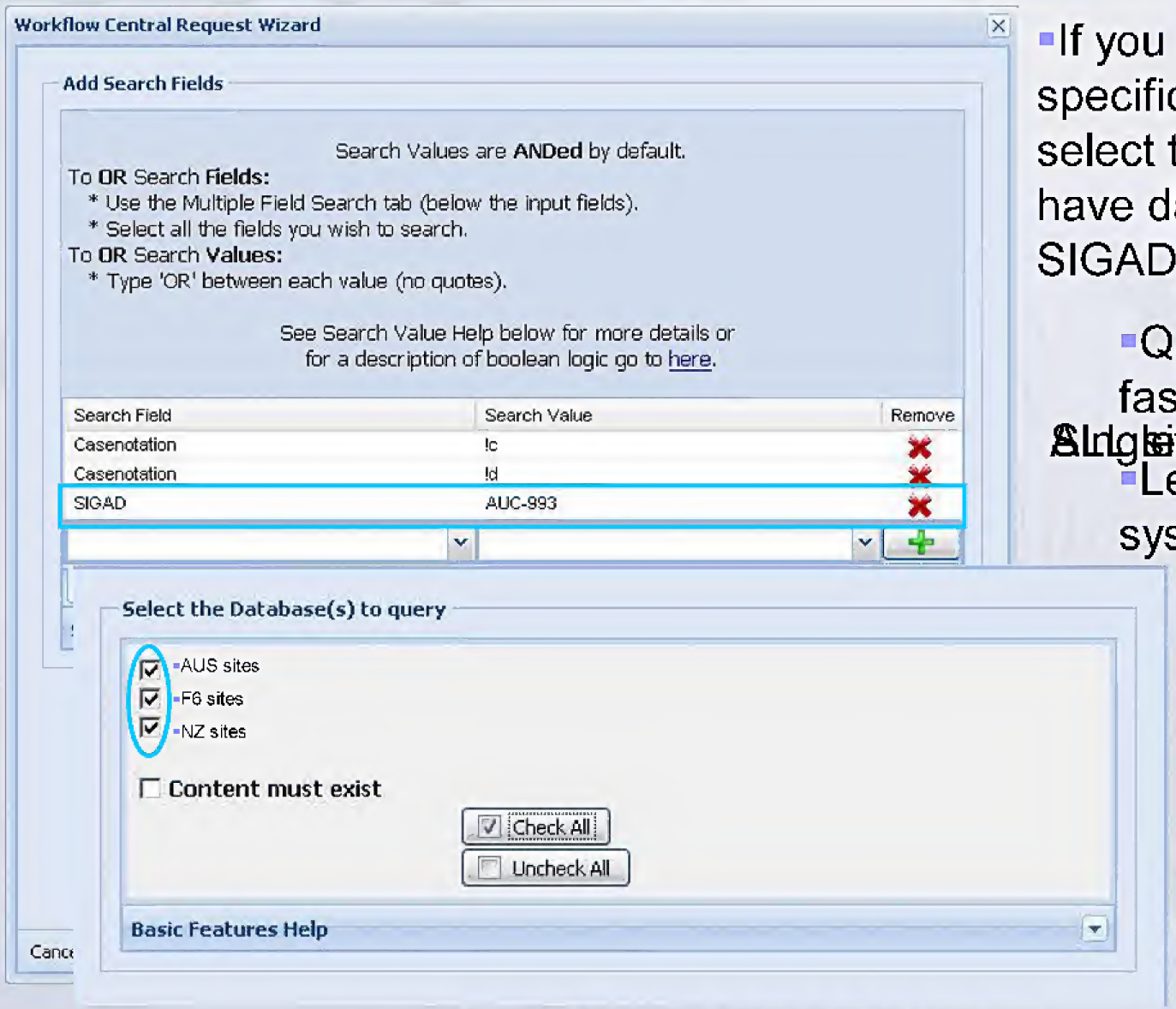


Common mistakes

- This will return ALL casenotations.
  - a will be deafeted by “!a” but a does equal “!b”
- All the defeated values must be ANDed together.



Common mistakes



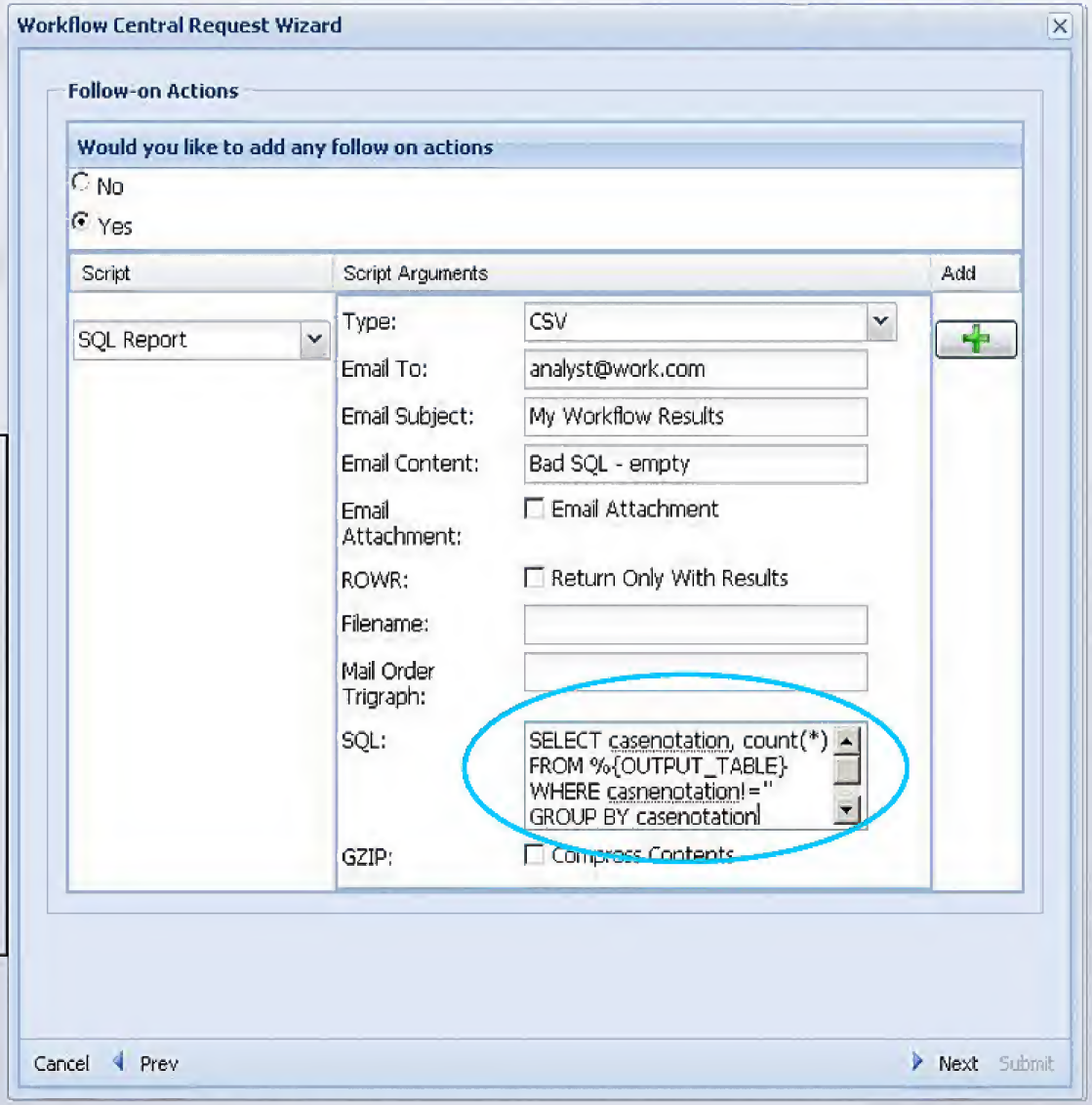
- If you are selecting specific SIGADs, only select the sites that have data from that SIGAD.
  - Queries will return faster.
  - Less work for the system.

Common mistakes

- If you select the SQL Report option, make sure you put a valid SQL statement!

SQL statement filled in:

```
SELECT casenotation, count(*)
FROM %{OUTPUT_TABLE}
WHERE casenotation!=''
GROUP BY casenotation
```



Questions?

xks_workflow@r1.r.nsa